CompTIA PenTest+ Certification Exam Objectives

EXAM NUMBER: PT0-002

About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA PenTest+ (PT0-002) certification exam. The CompTIA PenTest+ certification exam will verify the successful candidate has the knowledge and skills required to:

- **Plan and scope a penetration testing engagement**
- **Understand legal and compliance requirements**
- **Perform vulnerability scanning and penetration testing using appropriate tools and techniques, and then analyze the results**
- **Produce a written report containing proposed remediation techniques, effectively communicate results to the management team, and provide practical recommendations**

This is equivalent to three to four years of hands-on experience working in a security consultant or penetration tester job role.

These content examples are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

EXAM ACCREDITATION

The CompTIA PenTest+ (PT0-002) exam is accredited by ANSI to show compliance with the ISO 17024 standard and, as such, undergoes regular reviews and updates to the exam objectives.

EXAM DEVELOPMENT

CompTIA exams result from subject-matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

CompTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka "brain dumps"). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA's exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the **CompTIA Certification Exam Policies**. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the **CompTIA Candidate Agreement**. If a candidate has a question as to whether study materials are considered unauthorized (aka "brain dumps"), he/she should contact CompTIA at **examsecurity@comptia.org** to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	PT0-002
Number of questions	Maximum of 85
Types of questions	Multiple-choice and performance-based
Length of test	165 minutes
Recommended experience	3–4 years of hands-on experience performing penetration tests, vulnerability assessments, and code analysis
Passing score	750 (on a scale of 100-900)

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Planning and Scoping	14%
2.0 Information Gathering and Vulnerability Scanning	22%
3.0 Attacks and Exploits	30%
4.0 Reporting and Communication	18%
5.0 Tools and Code Analysis	16%
Total	**100%**

1.0 Planning and Scoping

1.1 Compare and contrast governance, risk, and compliance concepts.

- **Regulatory compliance considerations**
  - Payment Card Industry Data Security Standard (PCI DSS)
  - General Data Protection Regulation (GDPR)
- **Location restrictions**
  - Country limitations
  - Tool restrictions
  - Local laws
  - Local government requirements
    - Privacy requirements
- **Legal concepts**
  - Service-level agreement (SLA)
  - Confidentiality
  - Statement of work
  - Non-disclosure agreement (NDA)
  - Master service agreement
- **Permission to attack**

1.2 Explain the importance of scoping and organizational/customer requirements.

- **Standards and methodologies**
  - MITRE ATT&CK
  - Open Web Application Security Project (OWASP)
  - National Institute of Standards and Technology (NIST)
  - Open-source Security Testing Methodology Manual (OSSTMM)
  - Penetration Testing Execution Standard (PTES)
  - Information Systems Security Assessment Framework (ISSAF)
- **Rules of engagement**
  - Time of day
  - Types of allowed/disallowed tests
  - Other restrictions
- **Environmental considerations**
  - Network
  - Application
  - Cloud
- **Target list/in-scope assets**
  - Wireless networks
  - Internet Protocol (IP) ranges
  - Domains
  - Application programming interfaces (APIs)
  - Physical locations
  - Domain name system (DNS)
  - External vs. internal targets
  - First-party vs. third-party hosted
- **Validate scope of engagement**
  - Question the client/review contracts
  - Time management
  - Strategy
    - Unknown-environment vs. known-environment testing

1.3 Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity.

- **Background checks of penetration testing team**
- **Adhere to specific scope of engagement**
- **Identify criminal activity**
- **Immediately report breaches/criminal activity**
- **Limit the use of tools to a particular engagement**
- **Limit invasiveness based on scope**
- **Maintain confidentiality of data/information**
- **Risks to the professional**
  - Fees/fines
  - Criminal charges

2.0 Information Gathering and Vulnerability Scanning

2.1 Given a scenario, perform passive reconnaissance.

- **DNS lookups**
- **Identify technical contacts**
- **Administrator contacts**
- **Cloud vs. self-hosted**
- **Social media scraping**
  - Key contacts/job responsibilities
  - Job listing/technology stack
- **Cryptographic flaws**
  - Secure Sockets Layer (SSL) certificates
  - Revocation
- **Company reputation/security posture**
- **Data**
  - Password dumps
  - File metadata
  - Strategic search engine analysis/enumeration
  - Website archive/caching
  - Public source-code repositories
- **Open-source intelligence (OSINT)**
  - Tools
    - Shodan
    - Recon-ng
  - Sources
    - Common weakness enumeration (CWE)
    - Common vulnerabilities and exposures (CVE)

2.2 Given a scenario, perform active reconnaissance.

- **Enumeration**
  - Hosts
  - Services
  - Domains
  - Users
  - Uniform resource locators (URLs)
- **Website reconnaissance**
  - Crawling websites
  - Scraping websites
  - Manual inspection of web links
    - robots.txt
- **Packet crafting**
  - Scapy
- **Defense detection**
  - Load balancer detection
  - Web application firewall (WAF) detection
  - Antivirus
  - Firewall
- **Tokens**
  - Scoping
  - Issuing
  - Revocation
- **Wardriving**
- **Network traffic**
  - Capture API requests and responses
  - Sniffing
- **Cloud asset discovery**
- **Third-party hosted services**
- **Detection avoidance**

2.3 Given a scenario, analyze the results of a reconnaissance exercise.

- **Fingerprinting**
  - Operating systems (OSs)
  - Networks
  - Network devices
  - Software
- **Analyze output from:**
  - DNS lookups
  - Crawling websites
  - Network traffic
  - Address Resolution Protocol (ARP) traffic
  - Nmap scans
  - Web logs

2.4 Given a scenario, perform vulnerability scanning.

- **Considerations of vulnerability scanning**
  - Time to run scans
  - Protocols
  - Network topology
  - Bandwidth limitations
  - Query throttling
  - Fragile systems
  - Non-traditional assets
- **Scan identified targets for vulnerabilities**
- **Set scan settings to avoid detection**
- **Scanning methods**
  - Stealth scan
  - Transmission Control Protocol (TCP) connect scan
  - Credentialed vs. non-credentialed
- **Nmap**
  - Nmap Scripting Engine (NSE) scripts
  - Common options
    - -A
    - -sV
    - -sT
    - -Pn
    - -O
    - -sU
    - -sS
    - -T 1-5
    - -script=vuln
    - -p
- **Vulnerability testing tools that facilitate automation**

3.0 Attacks and Exploits

3.1 Given a scenario, research attack vectors and perform network attacks.

- **Stress testing for availability**
- **Exploit resources**
  - Exploit database (DB)
  - Packet storm
- **Attacks**
  - ARP poisoning
  - Exploit chaining
  - Password attacks
    - Password spraying
    - Hash cracking
    - Brute force
    - Dictionary
  - On-path (previously known as man-in-the-middle)
  - Kerberoasting
  - DNS cache poisoning
  - Virtual local area network (VLAN) hopping
  - Network access control (NAC) bypass
  - Media access control (MAC) spoofing
  - Link-Local Multicast Name Resolution (LLMNR)/NetBIOS-Name Service (NBT-NS) poisoning
  - New Technology LAN Manager (NTLM) relay attacks
- **Tools**
  - Metasploit
  - Netcat
  - Nmap

3.2 Given a scenario, research attack vectors and perform wireless attacks.

- **Attack methods**
  - Eavesdropping
  - Data modification
  - Data corruption
  - Relay attacks
  - Spoofing
  - Deauthentication
  - Jamming
  - Capture handshakes
  - On-path
- **Attacks**
  - Evil twin
  - Captive portal
  - Bluejacking
  - Bluesnarfing
  - Radio-frequency identification (RFID) cloning
  - Bluetooth Low Energy (BLE) attack
  - Amplification attacks [Near-field communication (NFC)]
  - WiFi protected setup (WPS) PIN attack
- **Tools**
  - Aircrack-ng suite
  - Amplified antenna

3.3 Given a scenario, research attack vectors and perform application-based attacks.

- **OWASP Top 10**
- **Server-side request forgery**
- **Business logic flaws**
- **Injection attacks**
    - Structured Query Language (SQL) injection
        - Blind SQL
        - Boolean SQL
        - Stacked queries
    - Command injection
    - Cross-site scripting
        - Persistent
        - Reflected
    - Lightweight Directory Access Protocol (LDAP) injection
- **Application vulnerabilities**
    - Race conditions
    - Lack of error handling
    - Lack of code signing
    - Insecure data transmission
    - Session attacks
        - Session hijacking
        - Cross-site request forgery (CSRF)
        - Privilege escalation
        - Session replay
        - Session fixation
- **API attacks**
    - Restful
    - Extensible Markup Language-Remote Procedure Call (XML-RPC)
    - Soap
- **Directory traversal**
- **Tools**
    - Web proxies
        - OWASP Zed Attack Proxy (ZAP)
        - Burp Suite community edition
    - SQLmap
    - DirBuster
- **Resources**
    - Word lists

3.4 Given a scenario, research attack vectors and perform attacks on cloud technologies.

- **Attacks**
    - Credential harvesting
    - Privilege escalation
    - Account takeover
    - Metadata service attack
    - Misconfigured cloud assets
        - Identity and access management (IAM)
        - Federation misconfigurations
        - Object storage
        - Containerization technologies
    - Resource exhaustion
    - Cloud malware injection attacks
    - Denial-of-service attacks
    - Side-channel attacks
    - Direct-to-origin attacks
- **Tools**
    - Software development kit (SDK)

3.5 Explain common attacks and vulnerabilities against specialized systems.

- **Mobile**
    - Attacks
        - Reverse engineering
        - Sandbox analysis
        - Spamming
    - Vulnerabilities
        - Insecure storage
        - Passcode vulnerabilities
        - Certificate pinning
        - Using known vulnerable components
            - (i) Dependency vulnerabilities
            - (ii) Patching fragmentation
        - Execution of activities using root
        - Over-reach of permissions
        - Biometrics integrations
        - Business logic vulnerabilities
    - Tools
        - Burp Suite
        - Drozer
        - Mobile Security Framework (MobSF)
        - Postman
        - Ettercap
        - Frida
        - Objection
        - Android SDK tools
        - ApkX
        - APK Studio
- **Internet of Things (IoT) devices**
    - BLE attacks
    - Special considerations
        - Fragile environment
        - Availability concerns
        - Data corruption
        - Data exfiltration
    - Vulnerabilities
        - Insecure defaults
        - Cleartext communication
        - Hard-coded configurations
        - Outdated firmware/hardware
        - Data leakage
        - Use of insecure or outdated components
- **Data storage system vulnerabilities**
    - Misconfigurations—on-premises and cloud-based
        - Default/blank username/password
        - Network exposure
    - Lack of user input sanitization
    - Underlying software vulnerabilities
    - Error messages and debug handling
    - Injection vulnerabilities
        - Single quote method
- **Management interface vulnerabilities**
    - Intelligent platform management interface (IPMI)
- **Vulnerabilities related to supervisory control and data acquisition (SCADA)/ Industrial Internet of Things (IIoT)/ industrial control system (ICS)**
- **Vulnerabilities related to virtual environments**
    - Virtual machine (VM) escape
    - Hypervisor vulnerabilities
    - VM repository vulnerabilities
- **Vulnerabilities related to containerized workloads**

3.6 Given a scenario, perform a social engineering or physical attack.

- **Pretext for an approach**
- **Social engineering attacks**
    - Email phishing
        - Whaling
        - Spear phishing
    - Vishing
    - Short message service (SMS) phishing
    - Universal Serial Bus (USB) drop key
    - Watering hole attack
- **Physical attacks**
    - Tailgating
    - Dumpster diving
    - Shoulder surfing
    - Badge cloning
- **Impersonation**
- **Tools**
    - Browser exploitation framework (BeEF)
    - Social engineering toolkit
    - Call spoofing tools
- **Methods of influence**
    - Authority
    - Scarcity
    - Social proof
    - Urgency
    - Likeness
    - Fear

3.7 Given a scenario, perform post-exploitation techniques.

- **Post-exploitation tools**
  - Empire
  - Mimikatz
  - BloodHound
- **Lateral movement**
  - Pass the hash
- **Network segmentation testing**
- **Privilege escalation**
  - Horizontal
  - Vertical
- **Upgrading a restrictive shell**
- **Creating a foothold/persistence**
  - Trojan
  - Backdoor
    - Bind shell
    - Reverse shell
  - Daemons
  - Scheduled tasks
- **Detection avoidance**
  - Living-off-the-land techniques/fileless malware
    - PsExec
    - Windows Management Instrumentation (WMI)
    - PowerShell (PS) remoting/Windows Remote Management (WinRM)
  - Data exfiltration
  - Covering your tracks
  - Steganography
  - Establishing a covert channel
- **Enumeration**
  - Users
  - Groups
  - Forests
  - Sensitive data
  - Unencrypted files

4.0 Reporting and Communication

4.1 Compare and contrast important components of written reports.

- **Report audience**
  - C-suite
  - Third-party stakeholders
  - Technical staff
  - Developers
- **Report contents (** not in a particular order)**
  - Executive summary
  - Scope details
  - Methodology
    - Attack narrative
  - Findings
    - Risk rating (reference framework)
    - Risk prioritization
    - Business impact analysis
  - Metrics and measures
  - Remediation
  - Conclusion
  - Appendix
- **Storage time for report**
- **Secure distribution**
- **Note taking**
  - Ongoing documentation during test
  - Screenshots
- **Common themes/root causes**
  - Vulnerabilities
  - Observations
  - Lack of best practices

4.2 Given a scenario, analyze the findings and recommend the appropriate remediation within a report.

- **Technical controls**
  - System hardening
  - Sanitize user input/ parameterize queries
  - Implemented multifactor authentication
  - Encrypt passwords
  - Process-level remediation
  - Patch management
  - Key rotation
  - Certificate management
  - Secrets management solution
  - Network segmentation
- **Administrative controls**
  - Role-based access control
  - Secure software development life cycle
  - Minimum password requirements
  - Policies and procedures
- **Operational controls**
  - Job rotation
  - Time-of-day restrictions
  - Mandatory vacations
  - User training
- **Physical controls**
  - Access control vestibule
  - Biometric controls
  - Video surveillance

4.3 Explain the importance of communication during the penetration testing process.

- **Communication path**
  - Primary contact
  - Technical contact
  - Emergency contact
- **Communication triggers**
  - Critical findings
  - Status reports
  - Indicators of prior compromise
- **Reasons for communication**
  - Situational awareness
  - De-escalation
  - Deconfliction
  - Identifying false positives
  - Criminal activity
- **Goal reprioritization**
- **Presentation of findings**

4.4 Explain post-report delivery activities.

- **Post-engagement cleanup**
  - Removing shells
  - Removing tester-created credentials
  - Removing tools
- **Client acceptance**
- **Lessons learned**
- **Follow-up actions/retest**
- **Attestation of findings**
- **Data destruction process**

5.0 Tools and Code Analysis

5.1 Explain the basic concepts of scripting and software development.

- **Logic constructs**
    - Loops
    - Conditionals
    - Boolean operator
    - String operator
    - Arithmetic operator
- **Data structures**
    - JavaScript Object Notation (JSON)
    - Key value
    - Arrays
    - Dictionaries
    - Comma-separated values (CSV)
    - Lists
    - Trees
- **Libraries**
- **Classes**
- **Procedures**
- **Functions**

5.2 Given a scenario, analyze a script or code sample for use in a penetration test.

- **Shells**
    - Bash
    - PS
- **Programming languages**
    - Python
    - Ruby
    - Perl
    - JavaScript
- **Analyze exploit code to:**
    - Download files
    - Launch remote access
    - Enumerate users
    - Enumerate assets
- **Opportunities for automation**
    - Automate penetration testing process
        - Perform port scan and then automate next steps based on results
        - Check configurations and produce a report
    - Scripting to modify IP addresses during a test
    - Nmap scripting to enumerate ciphers and produce reports

5.3 Explain use cases of the following tools during the phases of a penetration test.

*(**The intent of this objective is NOT to test specific vendor feature sets.)*

- **Scanners**
  - Nikto
  - Open vulnerability assessment scanner (Open VAS)
  - SQLmap
  - Nessus
  - Open Security Content Automation Protocol (SCAP)
  - Wapiti
  - WPScan
  - Brakeman
  - Scout Suite
- **Credential testing tools**
  - Hashcat
  - Medusa
  - Hydra
  - CeWL
  - John the Ripper
  - Cain
  - Mimikatz
  - Patator
  - DirBuster
  - w3af
- **Debuggers**
  - OllyDbg
  - Immunity Debugger
  - GNU Debugger (GDB)
  - WinDbg
  - Interactive Disassembler (IDA)
  - Covenant
  - SearchSploit
- **OSINT**
  - WHOIS
  - Nslookup
  - Fingerprinting Organization with Collected Archives (FOCA)
  - theHarvester
  - Shodan
  - Maltego
  - Recon-ng
  - Censys
- **Wireless**
  - Aircrack-ng suite
  - Kismet
  - Wifite2
  - Rogue access point
  - EAPHammer
  - mdk4
  - Spooftooph
  - Reaver
  - Wireless Geographic Logging Engine (WiGLE)
  - Fern
- **Web application tools**
  - OWASP ZAP
  - Burp Suite
  - Gobuster
- **Social engineering tools**
  - Social Engineering Toolkit (SET)
  - BeEF
- **Remote access tools**
  - Secure Shell (SSH)
  - Ncat
  - Netcat
  - ProxyChains
- **Networking tools**
  - Wireshark
  - Hping
- **Misc.**
  - SearchSploit
  - Responder
  - Impacket tools
  - Empire
  - Metasploit
  - mitm6
  - CrackMapExec
  - TruffleHog
  - Censys
- **Steganography tools**
  - Openstego
  - Steghide
  - Snow
  - Coagula
  - Sonic Visualiser
  - TinEye
- **Cloud tools**
  - Scout Suite
  - CloudBrute
  - Pacu
  - Cloud Custodian

PenTest+ (PT0-002) Acronym List

The following is a list of acronyms that appear on the CompTIA PenTest+ exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

ACRONYM	SPELLED OUT
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
AS2	Applicability Statement 2
BeEF	Browser Exploitation Framework
BLE	Bluetooth Low Energy
BSSID	Basic Service Set Identifiers
CA	Certificate Authority
CAPEC	Common Attack Pattern Enumeration and Classification
CLI	Command-Line Interface
CSRF	Cross-Site Request Forgery
CSV	Comma-Separated Values
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring Systems
CWE	Common Weakness Enumeration
DB	Database
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DLL	Dynamic Link Library
DLP	Data Loss Prevention
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EAP	Extensible Authentication Protocol
FOCA	Fingerprinting Organization with Collected Archives
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GDB	GNU Debugger
GDPR	General Data Protection Regulation
GPU	Graphics Processing Unit
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

ACRONYM	SPELLED OUT
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDA	Interactive Disassembler
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
IMEIs	International Mobile Equipment Identity
IoT	Internet of Things
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSAF	Information Systems Security Assessment Framework
JSON	JavaScript Object Notation
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LLMNR	Link-Local Multicast Name Resolution
LSASS	Local Security Authority Subsystem Service
MAC	Media Access Control
MDM	Mobile Device Management
MobSF	Mobile Security Framework
MOU	Memorandum of Understanding
MSA	Master Service Agreement
MX	Mail Exchange
NAC	Network Access Control
NBT-NS	NetBIOS Name Service
NDA	Non-disclosure Agreement
NFC	Near-Field Communication
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
NS	Name Server
NSE	Nmap Scripting Engine
NTLM	New Technology LAN Manager

ACRONYM	SPELLED OUT
NTP	Network Time Protocol
OS	Operating System
OSINT	Open-source Intelligence
OSSTMM	Open-source Security Testing Methodology Manual
OWASP	Open Web Application Security Project
PBKDF2	Password-Based Key Deviation Function 2
PCI DSS	Payment Card Industry Data Security Standard
PHP	PHP: Hypertext Preprocessor
PII	Personal Identifiable Information
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PS	PowerShell
PSK	Pre-Shared Key
PTES	Penetration Testing Execution Standard
RAT	Remote Access Trojan
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFC	Request for Comment
RFID	Radio-Frequency Identification
ROE	Rules of Engagement
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SDR	Software-defined Radio
SET	Social Engineering Toolkit
SGID	Set Group ID
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SLA	Service-level Agreement
SMB	Server Message Block
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SOW	Statement of Work
SQL	Structured Query Language
SSD	Solid-State Drive
SSH	Secure Shell
SSHD	Solid-State Hybrid Drive
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
SUID	Set User ID
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTL	Time to Live
TTPs	Tactics, Techniques and Procedures
UDP	User Datagram Protocol

ACRONYM	SPELLED OUT
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
USB	Universal Serial Bus
UTF	Unicode Transformation Format
VAS	Vulnerability Assessment Scanner
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VPS	Virtual Private Server
WAF	Web Application Firewall
WEP	Wired Equivalent Privacy
WiGLE	Wireless Geographic Logging Engine
WinRM	Windows Remote Management
WMI	Windows Management Instrumentation
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
XML-RPC	Extensible Markup Language-Remote Procedure Call
XSS	Cross-Site Scripting
ZAP	Zed Attack Proxy

PenTest+ Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the PenTest+ exam. This list may also be helpful for training companies that wish to create a lab component to their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

EQUIPMENT

- Laptops
- Wireless access points
- Servers
- Graphics processing units (GPUs)
- Switches
- Cabling
- Monitors
- Firewalls
- HID/door access controls
- Wireless adapters capable of packet injection
- Directional antenna
- Mobile device
- IoT equipment (cameras, Raspberry Pi, smart TV, etc.)
- Bluetooth adapter
- Access to cloud environment
  - Command-line interface (CLI) access
  - Management console access
  - Instances of cloud services
- Multifunction printers (wired/wireless enabled)
- Domain joined printer
- RFID readers
- Biometric device
- Programmable logic controller
  - Software-defined radio (SDR) kit
- USB flash drives
  - Weaponized USB drive

SPARE HARDWARE

- Cables
- Keyboards
- Mouse
- Power supplies
- Dongles/adapters

SPARE PARTS

- HDMI cables
- Spare hard drives
- Spare monitors

TOOLS

- Lock pick kit
- Badge cloner
- Fingerprint lifter
- Nail polish (to mask fingerprints)

SOFTWARE

- OS licensing
- Open-source OS
- Penetration testing frameworks
- VM software
- Scanning tools
- Credential testing tools
  - Spraying tools
  - Password crackers
- Debuggers
- Fuzzing tools
- Software assurance tools
- Wireless testing tools
- Web proxying tools
- Social engineering tools
- Remote access tools
- Network tools
- Mobility testing tools
- Security information and event management (SIEM)/intrusion detection system (IDS)/intrusion prevention system (IPS)
- Command and control tools
- Detection and avoidance tools